UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/734,310	12/12/2003	Leonard D. Rarick	SUNMP349	1691

32291 7590 09/12/2007
MARTINE PENILLA & GENCARELLA, LLP
710 LAKEWAY DRIVE
SUITE 200
SUNNYVALE, CA 94085

EXAMINER	
WANG, HARRIS C	

ART UNIT	PAPER NUMBER
2139	

MAIL DATE	DELIVERY MODE
09/12/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

MN

Office Action Summary	Application No.	Applicant(s)	
	10/734,310	RARICK ET AL.	
	Examiner	Art Unit	
	Harris C. Wang	2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 July 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) *16* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☐ Claim(s) *1-15 and 17-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *12 December 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1.

Claims 1, 14, 17 and 19 have been amended

Claim 16 has been cancelled

Claims 1-15 and 17-20 remain pending

Response to Arguments

Applicant's arguments with respect to claims 1-15, 17-20 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to

consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

Claims 1-10, 12, 14-20 rejected under 35 U.S.C. 103(a) as being unpatentable over Anand (20020191792) in view of Dworkin (7142669).

Regarding Claim 1,

Anand teaches a crypto algorithm unit comprising:

A first crypto hash execution module ; *(Fig. 1, MD5 circuit, 126)*

and a second crypto hash execution module, *(Fig. 1, SHA1 Circuit, 128)*

wherein the first crypto execution and the second crypto execution module share a plurality of components to form a combination crypto algorithm unit *("The system shares register and other circuit resources for MD5 and SHA1 hash circuits that are implemented in each hash channel" Abstract)*

Anand does not explicitly teach wherein the plurality of shared components include one or more adders, wherein each one of the one or more shared adders are included in the first crypto hash execution module and used to perform the first crypto hash execution and wherein each one of the one or more shared adders are included in the second crypto hash execution module and used to perform the second crypto hash execution.

Dworkin (7142669) teaches a plurality of shared components that includes a summing circuit wherein each one of the one or more adders are included in the first crypto hash execution module and used to perform the first crypto hash execution and wherein each one of the one or more shared adders are included in the second crypto hash execution module and used to perform the second crypto hash execution. *("A Message Digest Hardware Accelerator for implementing multiple cryptographic hash algorithms such as the Secure Hashing Algorithm 1 (SHA-1)…the Message Digest 5 (MD5) Algorithm….A function circuit performs logic operations based on the selected algorithm and provides the data value to a summing circuit (30) that is summed with mode dependent constant values selected from registers" Abstract)* The Examiner interprets the summing circuit as the adder and the first crypto execution hash module as the SHA-1 module and the second crypto execution hash module as the MD5 module.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the crypto algorithm unit of Anand with the method of using shared adders as taught by Dworkin.

The motivation is that Dworkin teaches sharing components such as adders is common when combining multiple cryptographic algorithms in a single hardware cryptographic execution unit.

Regarding Claim 2,

Anand teaches the crypto algorithm unit of claim 1, wherein the combination crypto algorithm unit includes a plurality of muxes. *("Hash block 103 comprises several multiplexers (indicated generally as "MUX") 202-214, Fig. 2)*

Regarding Claims 3 and 4,

Anand teaches the crypto algorithm unit of claim 2, wherein the plurality of muxes provides a crypto hash algorithm selection control, wherein the crypto hash algorithm selection control allows the selection of a first subset of the plurality of components, wherein the selected first subset of the plurality of components can execute a first crypto algorithm *("If a SHA1 hash is selected input (e.g. md5_sha1 is active or logic one), then the middle hash is selected. If an MD5 hash is selected (i.e. signal md5_sha1 is inactive or logic zero), then the first input md5_temp for mux 204 is selected" Paragraph [0118])*

Regarding Claim 5,

Anand teaches the crypto algorithm unit of claim 1, wherein the combination crypto algorithm unit is capable of executing at least two different crypto algorithms *("The system shares register and other circuit resources for MD5 and SHA1 hash circuits that are implemented in each hash channel" Abstract)*

Regarding Claim 6,

Anand teaches the crypto algorithm unit of claim 1, wherein the first crypto hash execution module is capable of executing at least one of a group of crypto hash algorithms consisting of an MD5 hash algorithm, a SHA-1 hash algorithm, a SHA256 hash algorithm, a SHA384 hash algorithm, and a SHA512 hash algorithm. *("The system shares register and other circuit resources for MD5 and SHA1 hash circuits that are implemented in each hash channel" Abstract)*

Regarding Claim 7,

Anand teaches the crypto algorithm unit of claim 6, wherein the second crypto hash execution module is capable of executing at least one of a group of crypto hash algorithms consisting of an MD5 hash algorithm, a SHA-1 hash algorithm, a SHA256 hash algorithm, a SHA384 hash algorithm, and a SHA512 hash algorithm that is different from the crypto hash algorithm that the first crypto hash execution module is capable of executing. *("The system shares register and other circuit resources for MD5 and SHA1 hash circuits that are implemented in each hash channel" Abstract)*

Regarding Claims 8 and 9,

Anand teaches the crypto algorithm unit of claim 1, wherein the combination crypto algorithm unit is on a single integrated circuit die. *("SHA1 algorithm is performed within an application specific integrated circuit (ASIC)…MD5 can be performed by software, or within an application specific integrated circuit (ASIC)" (Paragraph [0039] and Paragraph [0046])*

ASICs have microprocessor cores integrated in.

Regarding Claim 10,

Anand teaches the crypto algorithm unit of claim 1, wherein the combination crypto algorithm includes one or more full adders. *("The result is added, by a first full adder" Paragraph [0046])*

Regarding Claim 12,

Anand teaches the crypto algorithm unit of Claim 1, wherein the combination crypto algorithm unit includes one or more compressors. *("The result is added, by a first full adder" Paragraph [0046]).* The Examiner interprets a full adder as a 3 to 2 compressor.

Regarding Claims 14-18,

Anand teaches an integrated circuit comprising:

A microprocessor core; and a combination crypto algorithm unit, the combination crypto algorithm unit being coupled to the microprocessor core.

("SHA1 algorithm is performed within an application specific integrated circuit (ASIC)...MD5 can be performed by software, or within an application specific integrated circuit (ASIC)" (Paragraph [0039] and Paragraph [0046]). ASICs have microprocessor cores integrated in.

wherein the combination crypto algorithm unit is capable of executing at least two different crypto hash algorithms,

wherein the combination crypto algorithm unit includes a first crypto hash execution module and a second crypto hash execution module,

wherein the first crypto hash execution module is capable of executing at least one or a group of crypto hash algorithms consisting of an MD5 hash algorithm, a SHA-1 hash algorithm, a SHA256 hash algorithm, a SHA384 hash algorithm, and a SHA512 hash algorithm,

wherein the second crypto hash execution module is capable of executing at least one of a group of crypto hash algorithms consisting of an MD5 hash algorithm, a SHA-1 hash algorithm, a SHA256 hash algorithm, a SHA384 hash algorithm, and a SHA512 hash algorithm that is different from the crypto hash algorithm that the first crypto hash execution is capable of executing.

("The system shares register and other circuit resources for MD5 and SHA1 hash circuits that are implemented in each hash channel" Abstract)

The Examiner interprets the first execution module as SHA1 and the second as MD5.

Anand does not explicitly teach wherein the plurality of shared components include one or more adders, wherein each one of the one or more shared adders are included in the first crypto hash execution module and used to perform the first crypto hash execution and wherein each one of the one or more shared adders are included in the second crypto hash execution module and used to perform the second crypto hash execution.

Dworkin (7142669) teaches a plurality of shared components that includes a summing circuit wherein each one of the one or more adders are included in the first crypto hash execution module and used to perform the first crypto hash execution and wherein each one of the one or more shared adders are included in the second crypto hash execution module and used to perform the second crypto hash execution. *("A Message Digest Hardware Accelerator for implementing multiple cryptographic hash algorithms such as the Secure Hashing Algorithm 1 (SHA-1)...the Message Digest 5 (MD5) Algorithm....A function circuit performs logic operations based on the selected algorithm and provides the data value to a summing circuit (30) that is summed with mode dependent constant values selected from registers" Abstract)* The Examiner interprets the summing circuit as the adder and the first crypto execution hash module as the SHA-1 module and the second crypto execution hash module as the MD5 module.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the crypto algorithm unit of Anand with the method of using shared adders as taught by Dworkin.

The motivation is that Dworkin teaches sharing components such as adders is common when combining multiple cryptographic algorithms in a single hardware cryptographic execution unit.

Regarding Claims 19-20,

Anand teaches a method of executing a crypto instruction comprising:

Receiving a first crypto hash instruction in a combination crypto algorithm unit;

Determining a corresponding first crypto hash algorithm for the first crypto instruction;

Selecting a first plurality of components in the combination crypto algorithm unit; and

Executing the first crypto hash instruction through the selected first plurality of components.

("If a SHA1 hash is selected input (e.g. md5_sha1 is active or logic one), then the middle hash is selected. If an MD5 hash is selected (i.e. signal md5_sha1 is inactive or logic zero), then the first input md5_temp for mux 204 is selected" Paragraph [0118])

Receiving a second crypto hash instruction in the combination crypto algorithm unit;

Determining a corresponding second crypto hash algorithm for the second crypto hash instruction

Selecting a second plurality of components in the combination crypto algorithm unit; and executing the second crypto hash instruction through the selected second plurality of components,

("If a SHA1 hash is selected input (e.g. md5_sha1 is active or logic one), then the middle hash is selected. If an MD5 hash is selected (i.e. signal md5_sha1 is inactive or logic zero), then the first input md5_temp for mux 204 is selected" Paragraph [0118])

the selected second plurality of components and the selected first plurality of components sharing a third plurality of components. (Fig. 1, shows the MD5 circuit and the SHA1 sharing circuitry)

The Examiner interprets the first crypto algorithm as SHA1 and the second as MD5. In order to select a hash input, it is inherent that an instruction must first be received. Furthermore it is inherent that after a hash algorithm is selected the hash instruction will execute.

Anand does not explicitly teach wherein the plurality of shared components include one or more adders, wherein each one of the one or more shared adders are included in the first crypto hash execution module and used to perform the first crypto hash execution and wherein each one of the one or more shared adders are included in the second crypto hash execution module and used to perform the second crypto hash execution.

Dworkin (7142669) teaches a plurality of shared components that includes a summing circuit wherein each one of the one or more adders are included in the first

crypto hash execution module and used to perform the first crypto hash execution and wherein each one of the one or more shared adders are included in the second crypto hash execution module and used to perform the second crypto hash execution. *("A Message Digest Hardware Accelerator for implementing multiple cryptographic hash algorithms such as the Secure Hashing Algorithm 1 (SHA-1)...the Message Digest 5 (MD5) Algorithm....A function circuit performs logic operations based on the selected algorithm and provides the data value to a summing circuit (30) that is summed with mode dependent constant values selected from registers" Abstract)* The Examiner interprets the summing circuit as the adder and the first crypto execution hash module as the SHA-1 module and the second crypto execution hash module as the MD5 module.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the crypto algorithm unit of Anand with the method of using shared adders as taught by Dworkin.

The motivation is that Dworkin teaches sharing components such as adders is common when combining multiple cryptographic algorithms in a single hardware cryptographic execution unit.

Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over Anand and Dworkin in view of Qi (US 20020184498).

Regarding Claim 11,

Anand and Dworkin teaches the crypto algorithm unit of claim 1. Anand does not explicitly teach wherein the combination crypto algorithm unit includes one or more carry look-ahead adders.

Qi teaches a combination crypto algorithm unit includes one or more carry look-ahead adders. *("combination crypto algorithm unit includes one or more carry look-ahead adders." Paragraph [0014])*

It would have been obvious to one of ordinary skill in the art at the time of the invention to use carry look-ahead adders

The motivation to include carry look ahead adders is because CLAs are faster than ripple carry adders.

Claim 13 is rejected under 35 U.S.C. 103(a) as being unpatentable over Anand and Dworkin in view of Bradley (6711633).

Regarding Claim 13,

Anand and Dworkin teaches the crypto algorithm unit of claim 12. Anand does not explicitly teach wherein the one or more compressors includes a group of a 4 to 2 compressor.

Bradley teaches "a CSA is referred to herein as a 3:2 compressor...for wide operands, however, the number of stages of 3:2 compressors required may result in

excessive propagation delay. To address this problem, so-called 4:2 compressors have been used to reduce the propagation delay by reducing the number of stages." (Column 1, lines 42-50)

It would have been obvious to one of ordinary skill in the art at the time of the invention to include 4:2 compressors in the system of Anand.

The motivation is to reduce the propagation delay by reducing the number of stages.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Harris C. Wang whose telephone number is 5712701462. The examiner can normally be reached on M-F 8-5:30, Alternate Fridays Off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, AYAZ R. SHEIKH can be reached on (571)272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

HCW

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100